

Serial No. 09/468,377
Art Unit No. 2134

REMARKS

Claims 1-17 are currently pending in the patent application. The Examiner has finally rejected Claims 1, 5, 12, 13, 15 and 16 under 35 USC 103 as unpatentable over the teachings of Thomlinson in view of Shi; Claims 2 and 6 as unpatentable in view of Thomlinson in view of Shi and Danneels; Claims 3 and 7 as unpatentable over Thomlinson in view of Shi and Buck; Claims 4 and 8 as unpatentable over Thomlinson in view of Shi and the IBM TDB; Claims 9-11, 14, and 17 as unpatentable over Jablon in view of Thomlinson; and, Claim 11 as being unpatentable over the teachings of Jablon and Thomlinson in view of Schneider. For the reasons set forth below, Applicants respectfully assert that all of the pending claims are patentable over the cited prior art.

The present invention is a computer program product and method for securely providing data of a content provider to a user without trusting an internet service provider. As Applicants had previously argued, the present invention allows secure data transfer between a content provider and a user without having the internet service provider participate in the security features. In that way, a user

YO999-558

-12-

Serial No. 09/468,377
Art Unit No. 2134

could access the internet through any service provider, without sharing any security information with the internet service provider. Similarly, the content provider could secure transmit data to a trusted user, without concern that the internet service provider, or other customers of the internet service provider, could access the content provider's data. The security relationship is between the content provider and the user. What is critical to understand in this scenario is that the internet service provider and the content provider are two distinctly different entities.

The claims expressly recite steps for exchanging encryption keys and passwords only between the user and the content provider. By the present amendments, Applicants have ensured that all of the claims expressly recite that the content provider is not the internet service provider and that the secure transmission is done without trusting the internet service provider.

The Examiner stated in the *Response to Arguments* section that the Thomlinson reference teaches "only two entities (user and provider) involved with establishing encryption and authentication processes." Applicants wish

YO999-558

-13-

Serial No. 09/468,377
Art Unit No. 2134

to point out that the two entities in the Thomlinson patent are the user and the single server/service provider. As expressly stated in Col. 2, lines 12-13 of Thomlinson, "encryption is based on the user's logon password or some other secret supplied during network logon." Applicants contend that the security relationship in the Thomlinson patent is not between a user and a content provider wherein the content provider is a different entity from the service provider. The Thomlinson patent is directed to a system and method for protecting data wherein the service provider is involved in the encryption and authentication process. Applicants respectfully assert that the present invention expressly omits the service provider from the process in order to protect data when an untrusted service provider is part of the data delivery.

Applicants have further argued that the Thomlinson keys are reversed from that which is taught and claimed by the present invention. Whereas Thomlinson uses a first master key to encrypt a second item key, and then uses the first master key to decrypt the second key for a user to access the item data, the present invention does not use the second key to encrypt stored items. Rather, the present invention

YO999-558

-14-

Serial No. 09/468,377
Art Unit No. 2134

creates the second key and stores that encrypted second key at the client machine. In response to the foregoing argument, the Examiner has stated that "the present invention claims two keys, a first key known only to the *service provider* and a second key that is encrypted using the first key and a one-time password and is then stored on the client machine (*emphasis added*)."

Applicants respectfully assert that the Examiner is incorrect in stating the claim language since the claims explicitly state that a first key, or a component "b", is known only to the content provider, which is a different entity from the service provider. Clearly the Examiner misstated the language of the claims.

Moreover, the Examiner further argues that the item key of Thomlinson reads on the second key. However, Thomlinson states at Col. 9, lines 13-27 that "an item key is randomly generated for each data item received...[and]...[t]he data item is encrypted with its corresponding item key...using a master key." Further, "the master key is encrypted using a code that is derived from user authentication." Clearly what Thomlinson is teaching is encryption based on user identification at logon, using an encryption algorithm which

Y0999-558

-15-

Serial No. 09/468,377
Art Unit No. 2134

was previously determined (see: Col. 8, lines 64-67), and assignment of item "keys", which are not encryption or decryption keys but are item identifiers that are encrypted along with the items. Clearly Thomlinson is not teaching or suggesting generating first and second keys as claimed.

Finally with regard to the fact that Thomlinson uses their key to encrypt data, Applicants again note that Thomlinson encrypts data using a key. What the present invention claims is decrypting the second key to access data. The claims do not recite decrypting data with the key, they recite accessing data with the decrypted key.

As acknowledged by the Examiner, the Thomlinson patent does not teach or suggest storing encrypted second keys at the client. What the Examiner says is that the cookies created and stored at the client in the Shi patent render that claim feature obvious. Applicants respectfully assert that the Shi cookies are not the same as or suggestive of an encrypted second key which is encrypted using a first key known only to the content provider and is sent for storage at a client. A cookie as detailed in Shi is a non-unique, non-encrypted, fully accessible set of data which can be replicated on any client machine which accesses a server.

YO999-558

-16-

Serial No. 09/468,377
Art Unit No. 2134

In contrast, when Applicants teach that "an encrypted opaque cookie is stored on the client's machine for future accesses," Applicants are clearly not referring to the same type of stored data. Storing a Shi cookie is unworkable for an authentication system in which access is to be limited. Moreover, even if one skilled in the art were to modify Thomlinson with the Shi cookies, one would not arrive at the present invention.

The other primary reference, Jablon, provides a scheme in which two trusted parties each generate a unique code and share it. The Jablon patent does not, however, teach or suggest the particular code generation scheme which is taught and claimed by the claims including 9-11 and 14 and 17. The claims are not drawn to "a method wherein two parties operate on the same code element", but are quite specific to the implementation claimed. Accordingly, Applicants believe that the Jablon teachings do not obviate the invention as claimed. The Examiner has argued that Jablon teaches the steps set forth in independent Claims 9, 14 and 17. However, what the cited Jablon teachings describe is that Bob and Alice both compute the same value of K using independently-selected values of R_B and R_A .

YO999-558

-17-

Serial No. 09/468,377
Art Unit No. 2134


respectively (see: Col. 4, line 66-Col. 5, line 7. Clearly it cannot be maintained that the Jablon teachings of calculating an identical value of K obviates the claimed steps of calculating $g^{(a*b)}$ by said client machine using the one-time password to decrypt encrypted g^b ; and transmitting $g^{(a*b)}$ to the content provider, whereby the client machine's knowledge of $g^{(a*b)}$ authenticates the user to the content provider.

Based on the foregoing amendments and remarks, Applicants respectfully request entry of the amendments, reconsideration of the amended claim language in light of the remarks, withdrawal of the rejections, and allowance of the claims.

Respectfully submitted,

Y. Baransky, et al

By:


Anne Vachon (Dougherty)
Registration No. 30,374
Tel. (914) 962-5910

YO999-558

-18-